

MANAGEMENT OF SECURITY KEY DISTRIBUTION

ABSTRACT

5

Security keys for the provision of a secure service such as content provision are generated in an ancestral hierarchy, so that invalidation of a key in the hierarchy results in a need to reconfigure all other keys in the hierarchy to the extent they share common ancestry. When a user subscription to the service lapses, a decision on
10 invalidation of their key is based in a determination of whether it's more costly to the subscriber to invalidate the key, or continue providing an unpaid-for service. Keys can be allocated to users from domains of the hierarchy on the basis of their economic value to the provider, with higher value users being allocated keys from domains which share fewer common ancestors with other users of other domains than those
15 users share with each other, to minimise inconvenience to high value users of key reconfiguration.